PATENT Docket No. 29250-000161

IN THE U.S. PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

Applicant:	Sarvar PATEL	Conf. No.:	1713
Appl. No.:	09/127,767	Group:	2132
Filed:	February 23, 2000	Examiner:	S. Kabakoff

For: METHOD FOR TWO PARTY AUTHENTICATION AND KEY AGREEMENT

BRIEF ON BEHALF OF APPELLANT
FILED UNDER PROVISIONS OF 37 C.F.R. § 1.192

Assistant Commissioner for Patents
Washington, D.C. 20231

Date: March 4, 2002

TABLE OF CONTENTS

I.	Real Party In Interest	Page 1
II.	Related Appeals and Interferences	Page 2
III.	Status of the Claims	Page 2
IV.	Status of Amendments	Page 2
V.	Summary of the Invention	Page 3
VI.	Issue Presented: Whether claims 1-22 are unpatentable under 35 U.S.C. § 103(a) over Menezes et al.	Page 9
VII.	Grouping of Claims	Page 13
VIII.	Arguments	Page 14
	A. Group I	Page 14
	B. Group II	Page 17
	C. Group III	Page 19
	D. Group IV	Page 20
	E. Group V	Page 21
	F. Group VI	Page 23
	G. Group VII	Page 23
	H. Group VIII	Page 24
IX.	Conclusion	Page 24

Appendix of Claims attached.

PATENT
Docket No. 29250-000161

IN THE U.S. PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

Applicant:	Sarvar PATEL	Conf.:	1713
Appl. No.:	09/127,767	Group:	2132
Filed:	February 23, 2000	Examiner:	S. Kabakoff

For: METHOD FOR TWO PARTY AUTHENTICATION AND KEY AGREEMENT

DRAFT BRIEF ON BEHALF OF APPELLANT
FILED UNDER PROVISIONS OF 37 C.F.R. § 1.192

Assistant Commissioner for Patents
Washington, D.C. 20231

DATE: March 4, 2002

Sir:

This is an Appeal from the Final Rejection of May 11, 2001 of claims 1-22. This Appeal Brief is submitted in support of the Notice of Appeal filed on October 11, 2001, the period for response having been extended for three (3) months from December 11, 2001 to March 4, 2002.

I. REAL PARTY IN INTEREST

Appellant submits that the real party in interest in the present appeal is Lucent Technologies, Inc.

II. RELATED APPEALS AND INTERFERENCES

Appellant submits that no other appeals or interferences are known to Appellant, Appellant's legal representative, or the Assignee of the present application, which would directly affect or be directly affected by, or have a bearing on the Board's decision in the pending Appeal.

III. STATUS OF THE CLAIMS

Appellant submits that claims 1-22 are pending in the application. Claims 1 and 12 are independent claims. A complete copy of pending claims 1-22 is provided in the Appendix of Claims attached hereto.

Claims 1-22 stand rejected and are the claims on appeal.

IV. STATUS OF AMENDMENTS

Appellant filed a Response After Final with remarks (entry of which is requested). In an Advisory Action mailed September 27, 2001, the Examiner indicated that the arguments had been considered by were not persuasive. Appellant filed a Notice of Appeal on October 11, 2001, and is filing this Appeal Brief, in response to the final Office Action of May 11, 2001.

V. SUMMARY OF THE INVENTION

The present invention relates to a method for authenticating parties communicating with one another and executing a key agreement between the parties based on the authentication protocol.

Protocols for authenticating parties communicating with one another provide a measure of security to the communications. Such protocols form part of the different wireless communication standards in the U.S., Europe, and Japan. For example, the three major wireless systems used in the U.S., including TDMA, CDMA, and AMPS, all use the IS-41 standard defining the authentication procedure for call origination, updating secret shared data, etc. While the party authentication system and method of the present invention is not limited to wireless communication, the present invention will be described in the context of the IS-41 standard to facilitate understanding.

Fig. 1 illustrates a wireless system including an authentication center (AC) and a home location register (HLR) 10, a visiting location register (VLR) 15, and a mobile 20.

A root key, known as the A-key, is stored only in the AC/HLR 10 and the mobile 20. A secondary key, known as Shared Secret Data (SSD) is sent to the VLR 15 as the mobile 20 roams. The SSD is generated from the A-key and a random seed RANDSSD using a keyed cryptographic algorithm or function (KCF). The inputs to the KCF cannot

be determined from the outputs and knowledge of the KCF in use, unless the key is known.

The IS-41 protocol uses the Cellular Authentication and Voice Encryption (CAVE) as the KCF. When the mobile 20 roams, the VLR 15 in the area sends an authentication request to the AC/HLR 10, which responds by sending the mobile's SSD. Once the VLR has the SSD, it can independently authenticate the mobile 20. For security reasons, the SSD is periodically updated.

Fig. 2 illustrates the communication between the AC/HLR 10, the VLR 15, and the mobile 20 to update the SSD. The AC/HLR 10 generates a random number seed RANDSSD, and generates a new SSD using the CAVE algorithm and RANDSSD. After receiving the new SSD and RANDSSD, the VLR 15 sends the RANDSSD to the mobile 20 along with a session request SR, which instructs the mobile 20 to perform the SSD update protocol. In response, the mobile 20 uses the CAVE algorithm to generate the new SSD using the RANDSSD, and generates a random number R_M using a random number generator. The mobile 20 sends the random number R_M to the VLR 15. Also, the mobile performs the CAVE algorithm on the random number R_M using a portion of the new SSD as the key. This calculation is represented by $CAVE_{SSDA}(R_M)$.

Either the VLR 15 or AC/HLR 10 calculates $CAVE_{SSDA}(R_M)$, and sends the result to the mobile 20. The network is authenticated by the

mobile 20 if the $CAVE_{SSDA}(R_M)$ received from the network is the same as the $CAVE_{SSDA}(R_M)$ calculated by the mobile 20.

Next, the VLR 15 generates a random number R_N, calculates $CAVE_{SSDA}(R_N)$, and sends the R_N to the mobile 20. Upon receipt of R_N, the mobile 20 calculates $CAVE_{SSDA}(R_N)$, and sends the result to the VLR 15. The mobile 20 is authenticated by the VLR 15 if the two calculations of $CAVE_{SSDA}(R_N)$ match. The random number R_M and R_N are referred to as challenges, while $CAVE_{SSDA}(R_M)$ and $CAVE_{SSDA}(R_N)$ are challenge responses. Once authentication is complete, the mobile and the network generate session keys using the SSD.

In this protocol, the SSD itself is used to answer the challenges form the mobile 20 and the network. Thus, if an old RANDSSD and SSD pair is revealed to another party, this knowledge would be enough to query the mobile 20 and answer its challenge. Thus an attacker would be able to issue an SSD update to the mobile 20, and answer the mobile's challenge. Accordingly, an attacker would be able to impersonate the network and place a call to the mobile 20 under fraudulent identities. Such an attacker might pretend to be a credit card company, and ask to verify card number and pin.

The present invention is directed to a two party authentication method in which a first party issues a random number as a first challenge, and a second party responds with a first challenge response. The second party generates the first challenge response by performing a

keyed cryptographic function (KCF) on the first challenge and a generated count value using a first key. The second party sends the first challenge response to the first party, along with the generated count value, which is used as a second challenge.

The first party verifies the second party by performing the KCF on the first challenge and the generated count value, and matching the result of this calculation with the first challenge response. Then the first party uses the KCF to generate a second challenge response, which is sent to the second party for verification. An encryption key is then generated by both parties using the first and second challenges. In this manner, a different key, i.e., the first key, is used in answering challenges.

Fig. 3 illustrates the application of the present invention in the context of a wireless system. In this method, an M-key (first key) is generated by the AC/HLR 15 and the mobile 20 based on the A-key. For example, the M-key may be generated by applying a pseudo random function (PRF) indexed by the A-key on a value known to the network and the mobile 20.

As shown, the VLR 15 acts as a conduit between the AC/HLR 10 and the mobile 20. As shown, the AC/HLR 10 (first party) generates and sends a random number R_N (first challenge) to the mobile 20 (second party), along with a session request SR. In response, the mobile 20 generates a count value C_M, and performs a KCF on the first challenge

R_N, the count value C_M, type data, and id data ID_M using the M-key. This calculation is represented by $KCF_{M\text{-}Key}(Type, ID_M, C_M, R_N)$. The mobile increments the count value C_M prior to generating the challenge response $KCF_{M\text{-}Key}(Type, ID_M, C_M, R_N)$ to each challenge R_N from the network.

The Type data represents the type of protocol being performed, while the id data ID_M indicates that the communications whether the communication issued from the mobile 20 or the network. The inclusion of Type and ID_M data is specific to wireless applications, and is not required for two party authentication according to the present invention.

The mobile 20 sends the count value C_M and $KCF_{M\text{-}Key}(Type, ID_M, C_M, R_N)$ to the network (Type and ID_M is already known by the AC/HLR 10). The AC/HLR 10 also calculates $KCF_{M\text{-}Key}(Type, ID_M, C_M, R_N)$ and matches its calculation to the value received from the mobile 20. If a match is found, the mobile 20 is authenticated.

Next, the AC/HLR 10 uses the KCF and its own id data to generate the value of $KCF_{M\text{-}Key}(Type, ID_N, C_M)$ as a second challenge response. Meanwhile, the mobile 20 calculates the value of $KCF_{M\text{-}Key}(Type, ID_N, C_M, R_N)$ as well. This second challenge response is then sent from the AC/HLR to the mobile 20, so that the mobile 20 can verify the network by determining whether the calculated version of $KCF_{M\text{-}Key}(Type, ID_M, C_M, R_N)$ matches the received value.

After performing this two party authentication protocol, the mobile 20 and the AC/HLR 10 can generate the SSD using the first and second

challenges, i.e., R_N and C_N. For example, the mobile 20 and AC/HLR 10 can apply a pseudo random function (PRF) indexed by the A-key on the first and second challenges, thereby generating the SSD as $PRF_{A\text{-}Key}(C_M, R_N)$.

Since the present invention does not use a key previously established between the parties (e.g., A-key or SSD) to answer challenges during authentication, network impersonation by an attacker is not possible. Even if the first key (e.g., the M-key for IS-41 systems) is revealed to an attacker, the attacker has no direct way of obtaining the root key (A-key) therefrom, because a one-way function was used to generate the first key.

Further, if an attacker uses prior challenges and challenge responses to mount an attack, the attack will fail because the attacker will be using a challenge response based on an old count value. Consequently, neither the network nor the mobile 20 will verify the attacker. In addition, the attacker does not know the root key and therefore cannot obtain the keys which are generated after authentication by performing a PRF on the new challenge using the root key.

VI. ISSUE PRESENTED

Whether claims 1-22 are unpatentable under 35 U.S.C. § 103(a) over Menezes et al.

With respect to claim 1, the Examiner asserts that the Menezes et al. discloses the SKID3 algorithm in page 402. The Examiner asserts that according to SKID3, party A performs the following steps: (a) receives a random value r_B; (b) creates a new value r_A; (c) generates a response by performing a KCF on the received value r_B and the newly created value r_A; (d) transfers r_A and the generated response; (e) receives another response being a result of performing a KCF on the transferred value r_A; and (f) verifying the response received in step (e).

The Examiner states that the SKID3 algorithm only differs from the invention of claim 1 by using a value r_A instead of a "count value" as disclosed in the claim. The Examiner asserts that pages 397-400 of Menezes disclose three different types of numbers used in authentication protocols to prevent "replay" attacks: random numbers, sequence numbers, and timestamps. The Examiner further asserts that Menezes discloses the interchangeability in authentication protocols of random numbers, such as r_A, with sequence numbers, such as the count value in claim 1.

The Examiner alleges that it would have been obvious to one of ordinary skill in the art at the time the invention was made to replace the random number r_A in the SKID3 algorithm with a counter value, "since pages 397-400 of Menezes et al. disclose random numbers, sequence

numbers, serial numbers, counter values, and timestamps were all viable options known for preventing replay attacks in authentication protocols such as SKID3." See page 7, first full paragraph, of the Office Action issued on May 11, 2001 (hereafter Paper No. 6).

With respect to claim 2, the Examiner asserts that it was well known in the art at the time of the invention to generate a secondary key using an A-key as a root key. The Examiner further points to page 3, lines 20-26 of Appellant's present specification as describing such a prior art system with respect to Fig. 1. The Examiner states that it would have been obvious to one of ordinary skill in the art at the time the invention of the invention to use an A-key to generate key K in the SKID3 protocol of Menezes et al. since "this was a well known and often implemented method for effectively generating a cryptographic key in the art." (Page 8, second full paragraph, of Paper No. 6).

With respect to claim 3, the Examiner asserts that Menezes et al., page 402, discloses identification information "B" in SKID3.

With respect to claim 4, the Examiner asserts that Menezes et al. discloses a cryptographic key K, which is generated based on the protocol encrypting challenges r_A and r_B using the generated key K.

With respect to claim 5, the Examiner asserts that SKID3 could be used for authenticating a plurality of mobile units when r_B is broadcast globally from a single base unit (no citation to Menezes et al. is provided). The Examiner further asserts that page 3 of the Appellant's specification

describes a prior art authentication system comprising a base station and corresponding mobile stations, for which it would have been an obvious choice to use a well known authentication protocol such as SKID3 as described in Menezes et al.

With respect to claim 6, the Examiner asserts that the application of an authentication protocol to a wireless system was well known, as described by the admitted prior art system in page 3 of Appellant's present specification. The Examiner further asserts that one of ordinary skill in the art would know that a standard authentication protocol such as SKID3 could be implemented in a wireless environment such as that described in Appellant's admitted prior art system.

With respect to claim 7, the Examiner asserts that Menezes et al. disclose in page 402 identifiers "A" and "B," which are included in the generated responses. The Examiner further asserts that the identifiers allow a recipient to verify the identifier as his/her own, and optionally to embed additional random numbers in the identifier or to include information regarding the form of the challenges (bottom of page 401 of Menezes et al.).

According to the Examiner, since Menezes et al. teaches including information regarding "the form of the challenges" in identifiers included in a generated response, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include information pertaining to the form of challenges is the same as including protocol

information as recited in claim 7 "since a type of authentication protocol depends on the form of the challenges." See page 10, first paragraph, of Paper No. 6.

The Examiner asserts that claim 8 is unpatentable for the same reasons as claims 3 and 7. Further, the Examiner asserts that claim 9 is unpatentable for the same reasons as claim 4.

With respect to claim 10, the Examiner asserts that key K disclosed by Menezes et al. corresponds to a second key in the claimed invention (no citation to Menezes et al. is provided) where K is clearly a shared key since both parties A and B have access to it. Therefore, the Examiner asserts that the key K is shared secret data between A and B.

With respect to claim 11, the Examiner asserts that Menezes et al. teaches using a counter value in lieu of a random number to prevent replay attacks against an authentication protocol such as SKID3, for the reasons discussed with respect to claim 1. The Examiner admits that Menezes et al. does not explicitly teach a specific size or initialization procedure for generating a counter value.

The Examiner alleges that a 64 bit or greater counter value would have been an obvious design choice in the SKID3 authentication protocol when counter values of up to 2^{64} are required. The Examiner further alleges that the standard practice within the art to initialize a counter to start at some random offset value "to add an extra layer [of]

cryptographic security against potential reverse engineering of the authentication system.

With respect to claims 12-22, the Examiner alleges that these claims contain the same limitations as claims 1-11, "except from the point of view of the first party instead of from the point of view of the second party." (Page 11, first full paragraph, of Paper No. 6).

VII. GROUPING OF CLAIMS

Appellant respectfully requests that the following claims be grouped together as indicated:

Group I: Claims 12, 14, 15, and 18-20.

Group II: Claims 13 and 16.

Group III: Claim 17.

Group IV: Claims 21 and 22.

Group V: Claims 1-3, 5, 6, and 11.

Group VI: Claims 4 and 9.

Group VII: Claims 7 and 8.

Group VIII: Claim 10.

Appellant respectfully asserts that each of Groups I-IX are separately patentable for the reasons set forth below.

VIII. ARGUMENTS

A. Group I: Claims 12, 14, 15, and 18-20.

Independent claim 12 is directed to a method for authenticating a first party at a second part including the steps of outputting a random number as a first challenge, receiving a second challenge and a first challenge response, and verifying the first party based on the received first challenge, second challenge and first challenge response. Claim 12 recites that the second challenge is a count value, and that the first challenge response is a result of performing a keyed cryptographic function (KCF) on the first challenge and the count value using a first key.

In Section 6, pages 7-8, of Paper No. 6, the Examiner admits that the SKID3 algorithm disclosed by Menezes et al. fails to disclose a second challenge in the form of a count value. The Examiner states that SKID3 uses a random value r_A instead of a count value. However, the Examiner asserts that pages 397-400 of Menezes et al. teach interchangeability of authentication protocols of random numbers, such as r_A, with sequence numbers, such as the claimed count value (last paragraph of page 7).

The Examiner specifically asserts that Menezes et al. disclose three different types of numbers -- random numbers, sequence numbers, and timestamps -- used in authentication protocols to prevent "replay attacks." The Examiner states that one of ordinary skill in the art would have known "replay attacks were used to subvert challenge-response

authentication protocols, and therefore would have been familiar with choosing one of [random numbers, sequence numbers, and timestamps]" (top of page 8 of Paper No. 6).

The Examiner further alleges that it would have been obvious to one of ordinary skill in the art at the time of the invention to use a counter value instead of the random number r_A in the SKID3 protocol of Menezes et al, "since pages 397-400 of Menezes et al disclose random numbers, sequence numbers, serial numbers, counter values, and timestamps were all viable options known for preventing replay attacks in authentication protocols such as SKID3." (first full paragraph of page 8 in Paper No. 6).

Appellant respectfully submits that the Examiner has failed to provide the requisite showing of a teaching or motivation for his proposed modification, based on the evidence of record. In re Sang Su Lee, No. 00-1158, Slip Op. at 7-8; In re Dembiczak, 50 USPQ2d 1614 (Fed. Cir. 1999). The Examiner fails to point out a specific portion of Menezes et al., which would teach or motivate one to replace random numbers with sequence numbers (*i.e.*, count values) in the SKID3 authentication algorithm.

At most, the Examiner merely provides conclusory statements that one of ordinary skill would realize, in view of the teachings in pages 397-400, that a count value was a viable option to be used in the SKID3 algorithm. Appellant respectfully submits that the Examiner's

statements fail to specifically explain the reason *why* one of ordinary skill in the art would have specifically been led to the proposed modification, as required by Lee at 7-8. Instead, the Examiner merely states one of ordinary skill *could have* done so.

Further, contrary to the Examiner's assertions, Appellant respectfully submits that the Examiner's proposed modification to Menezes et al. fails to anticipate the present invention. Specifically, the use of the sequence number disclosed by Menezes et al. in a mutual authentication algorithm such as SKID3 would fail to anticipate the outputting of a first challenge, as required by claim 12.

Thus, Menezes et al. disclose the use of sequence numbers in challenge-response algorithms to perform one-pass authentication, in which only one message is sent between the parties during authentication because verifying party *does not send a first challenge to the party being authenticated.* This is described in page 401 of Menezes et al., under the heading: (i) Challenge-response based on symmetric-key encryption.

The use of sequence numbers, as disclosed by Menezes et al. requires each party to record and maintain long-term pair-wise state information regarding previously used and valid sequence numbers for each other party with which it communicates (page 399, Section 10.13). This substantial amount of overhead allows a verifying party to match the sequence number it expects to receive from the party requesting

authentication, with the sequence number actually received. Since Menezes et al. teaches that each party knows which sequence number will be used for verification, the verifying party does not issue this sequence number as a challenge to the party.

Accordingly, if the SKID3 algorithm of Menezes et al. were modified to use a sequence number instead of random number r_A, the resulting algorithm would omit message (1) shown on page 402. The Examiner's proposed modification would fail to disclose outputting a first challenge, and performing a keyed cryptographic function on both the count value and the first challenge, as required by claim 12. This modified SKID3 algorithm would therefore require substantially more overhead than the present invention.

Accordingly, reconsideration and withdrawal of this rejection is respectfully requested for the reasons set forth above. Appellant further respectfully submits that claims 14, 15, and 18-20 are allowable at least by virtue of their dependency on claim 12.

B. Group II: Claims 13 and 16

Claims 13 and 16 each recite establishing a second key based on the first and second challenges.

The Examiner asserts that it was well known in the art at the time the invention was made to generate a secondary key using an A-key as a root key. The Examiner points to page 3, lines 20-26, of Appellant's

present specification as describing such this feature in a prior art system. The Examiner alleges that it would have been obvious to one of ordinary skill in the art at the time the invention was made to use an A-key to generate key K in the SKID3 protocol of Menezes et al. "since this was a well known and often implemented method for effectively generating a cryptographic key." (page 8, second full paragraph, of Paper No. 6).

Appellant respectfully submits that the modification of the SKID3 algorithm of Menezes et al., as proposed by the Examiner, fails to anticipate the invention of claims 13 and 16. Specifically, both claims require that a second key to be established based on a first and second challenge, which is ignored by the Examiner's proposed modification.

In page 4 of Paper No. 6, the Examiner argues that the teachings of Menezes et al. read on the claimed invention because claim 13 does not require the "second key" to be a different key from the "first key," and that establishing a key "based" on the first and second challenges does not imply the first and second challenges are used to derive the key.

Appellant respectfully submits that by making these assertions, the Examiner is failing to interpret the words of each of claims 13 and 16 according to its plain meaning, as required by In re Zletz, 13 USPQ2d 1320, 1322 (Fed. Cir. 1989). The Examiner asserts that the claimed first key can also be interpreted as the second key of the claims. Not only does the Examiner fails to interpret claims 13 and 16 according to their

plain meaning, he refuses to ascribe *any meaning* to the words in the claims. Each of claims 13 and 16 requires two separate keys, one of which is established based on the first and second challenges.

Page 402 of Menezes et al. clearly teaches that h_K is a one way function of key K used to generate the first and second challenges. Since the key K is used in SKID3 *to generate the first and second challenges*, it cannot be construed as a second key established based on the first and second challenges, according to any reasonable interpretation.

Reconsideration and withdrawal of this rejection is therefore respectfully requested by Appellant.

C. Group III: Claim 17.

Claim 17 recites that the second key is one of a secret shared data and a session key.

In page 401, under the heading: (i) Challenge-response based on symmetric-key encryption, Menezes et al. teach that the SKID3 algorithm operates under the assumption of "the prior existence of a shared secret key." Since Menezes et al. disclose the existence of a secondary key (shared secret key) prior to the execution of SKID3, the reference clearly teaches away from establishing such a key based on first and second challenges exchanged during SKID3 authentication.

Accordingly, Appellant respectfully requests reconsideration and withdrawal of this rejection.

D. Group IV: Claims 21 and 22.

Claims 21 and 22 each recite the step of performing the KCF on the second challenge and type data, which indicates a type of protocol being performed by the network.

The Examiner points to the bottom of page 401 in Menezes et al. as teaching identifiers including information regarding "the form of the challenges." The Examiner further asserts that the inclusion of such information is the same as including the claimed protocol information since a type of authentication protocol depends on the form of the challenges.

Appellant respectfully submits that the Examiner has misconstrued the disclosure of Menezes et al. Specifically, the last paragraph of page 401 of Menezes et al. states, "[Party] *A* may...embed an additional random number in [its challenge response] *or, alternatively, the form of the challenges may be restricted.*" (emphasis added). Therefore, contrary to the Examiner's assertion, Menezes et al. provides absolutely no teaching of including information regarding the form of the challenge in its identifier in the challenge response $E_K(r_B, B^*)$. Rather, Menezes et al. disclose *restricting the form of the response* to be sent, *i.e.*, restricting the form of $E_K(r_B, B^*)$.

For the above reasons, Appellant respectfully submits that Menezes et al. fail to disclose performing a KCF on any data indicating a

type of protocol being performed. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

E. Group V: Claims 1-3, 5, 6, and 11.

Independent claim 1 recites a method for authenticating a first party at a second part including the steps of receiving a random number as a first challenge, incrementing a count value in response to receiving the first challenge, generating a first challenge response, transferring the first challenge response and the count value to the first party, receiving a second challenge response from the first party, and verifying the first party based on the second challenge and second challenge response. Claim 1 further recites that the first challenge response is a result of performing a keyed cryptographic function (KCF) on the first challenge and the count value using a first key.

The Examiner rejects claim 1 on the same grounds as independent claim 12. The Examiner's stated grounds of rejection are discussed above with respect to claim 12.

Appellant respectfully submits that independent claim 1 is allowable at least for the reasons discussed above with respect to independent claim 12. Specifically, Appellant respectfully submits that the Examiner's proposed modification of Menezes et al. is improper because the Examiner has failed to provide the requisite showing of a teaching or motivation for his proposed modification, based on the

evidence of record, as required by Lee. Further, the Examiner's proposed modification of Menezes et al. fails to anticipate the claimed features discussed above with respect to claim 12.

Appellant respectfully submit that claim 1 is further allowable because Menezes et al fails to provide any teaching or suggestion of incrementing a sequence number or count value in response to receiving a first challenge. In fact, Menezes et al. teach away from this feature.

As discussed above in connection with claim 12, Menezes et al. disclose the use of sequence number in challenge-response mechanisms like SKID3 to perform one-pass authentication, in which *no challenge is issued to a party to be authenticated.* See page 401 of Menezes et al. Accordingly, no first challenge would be received in the modified SKID3 algorithm using sequence numbers, which is proposed by the Examiner. Since the proposed modification of Menezes et al. fails to disclose the step of receiving a first challenge, it also fails to disclose the step of incrementing a count value in response to a received first challenge.

Accordingly, reconsideration and withdrawal of this rejection is respectfully requested for the above reasons. Appellant respectfully submit that claims 2, 3, 5, 6, and 11 are allowable at least by virtue of their dependency on claim 1.

F. Group VI: Claims 4 and 9.

Claims 4 and 9 each recite establishing a second key based on the first and second challenges. The Examiner rejects these claims on the same grounds as claims 13 and 16, discussed above.

Appellant respectfully submits that the Examiner's proposed modification of the SKID3 algorithm taught by Menezes et al. fails to teach or suggest this feature of claims 4 and 9, at least for the reasons discussed above with respect to claims 13 and 16.

Therefore, Appellant respectfully requests reconsideration and withdrawal of this rejection.

G. Group VII: Claims 7 and 8.

Claims 7 and 8 each recite the step of performing the KCF on the second challenge and type data, which indicates a type of protocol being performed by the network. The Examiner rejects these claims on the same grounds as claims 21 and 22.

Appellant respectfully submits that Menezes et al. fail to disclose the above claimed step at least for the reasons discussed above with respect to claims 21 and 22.

Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

H. Group VIII: Claim 10.

Claim 10 requires the second key to be one of a secret shared data and a session key. The Examiner rejects this claim on the same grounds as claim 17. The Examiner's grounds of rejection are discussed above with respect to claim 17.

Appellant respectfully submits that Menezes et al. actually teach away from the above features in claim 10, at least for the same reasons set forth above in connection to claim 17.

Reconsideration and withdrawal of this rejection is respectfully requested.

IX. CONCLUSION

For the reasons set forth above, it is respectfully submitted that all the claims in the application are allowable. Thus, favorable reconsideration and reversal of the Examiner's rejection of claims 1-22 is respectfully requested.

Should there be any outstanding matters which need to be resolved in the present application, the Board is respectfully requested to contact John A. Castellano, Registration No. 35,094 at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit of any overpayment to Deposit Account No. 08-0750 for any additional fees required by 37 C.F.R. §1.16 or under 37 C.F.R. §1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY & PIERCE, P.L.C.

By: _____

John A. Castellano
Registration No. 35,094
P.O. Box 8910
Reston, Virginia 20195
Telephone: (703) 390-3030

JAC:JWR

ATTACHED: APPENDIX OF CLAIMS

X. APPENDIX OF CLAIMS

Claim 1. A method for authenticating a first party at a second party, comprising:

(a) receiving a random number from said first party as a first challenge;

(b) incrementing a count value in response to receiving said first challenge;

(c) generating a first challenge response by performing a keyed cryptographic function (KCF) on said first challenge and said count value using a first key;

(d) transferring said count value, as a second challenge, and said first challenge response to said first party;

(e) receiving a second challenge response from said first party, said second challenge response being a result of performing said KCF on said second challenge using said first key; and

(f) verifying said first party based on said second challenge and said second challenge response.

Claim 2. The method of claim 1, prior to said step (c), further comprising:

(g) generating said first key using a root key.

Claim 3. The method of claim 1, wherein said step (c) generates said first challenge response by performing said KCF on said first challenge, said count value, and an identifier for said second party using said first key.

Claim 4. The method of claim 1, further comprising:

(g) establishing a second key based on said first and second challenges.

Claim 5. The method of claim 1, wherein said step (a) receives a global challenge as said first challenge from said first party.

Claim 6. The method of claim 1, wherein said first party is a network of a wireless system and said second party is a mobile.

Claim 7. The method of claim 6, wherein said step (c) generates said first challenge response by performing said KCF on said first challenge, said count value and type data using said first key, said type data indicating a type of protocol being performed by said network and said mobile.

Claim 8. The method of claim 6, wherein said step (c) generates said first challenge response by performing said KCF on said first

challenge, said count value, an identifier for said mobile, and type data using said first key, said type data indicating a type of protocol being performed by said network and said mobile.

Claim 9. The method of claim 6, further comprising:

(g) establishing a second key based on said first and second challenges.

Claim 10. The method of claim 9, wherein said second key is one of secret shared data and a session key.

Claim 11. The method of claim 6, wherein said step (b) increments said count value using a bit counter of greater than 64 bits and which was initialized using a random number.

Claim 12. A method for authenticating a first party at a second party, comprising:

(a) outputting a random number as a first challenge;

(b) receiving a second challenge and a first challenge response from said first party, said second challenge being a count value, and said first challenge response being a result of performing a keyed cryptographic function (KCF) on said first challenge and said count value using a first key; and

(e) verifying said first party based on said first challenge, said second challenge, and said first challenge response.

Claim 13. The method of claim 12, further comprising:

(f) establishing a second key based on said first and second challenges.

Claim 14. The method of claim 12, wherein said step (a) outputs said first challenge as a global challenge.

Claim 15. The method of claim 12, wherein said first party is a mobile of a wireless system and said second party is a network.

Claim 16. The method of claim 15, further comprising:

(f) establishing a second key based on said first and second challenges.

Claim 17. The method of claim 16, wherein said second key is one of secret shared data and a session key.

Claim 18. The method of claim 12, further comprising:

(f) generating a second challenge response by performing said KCF on said second challenge using said first key; and

(g) transferring said second challenge response to said second party.

Claim 19. The method of claim 18, wherein said step (f) generates said second challenge response by performing said KCF on said second challenge and an identifier for said second party using said first key.

Claim 20. The method of claim 18, wherein said first party is a mobile of a wireless system and said second party is a network.

Claim 21. The method of claim 20, wherein said step (f) generates said second challenge response by performing said KCF on said second challenge and type data using said first key, said type data indicating a type of protocol being performed by said network and said mobile.

Claim 22. The method of claim 20, wherein said step (f) generates said second challenge response by performing said KCF on said second challenge, an identifier for said network, and type data using said first key, said type data indicating a type of protocol being performed by said network and said mobile.

United States Court of Appeals for the Federal Circuit

00-1158
(Serial No. 07/631,240)

IN RE SANG SU LEE

Richard H. Stern, of Washington, DC, argued for Sang Su Lee. With him on the brief was Robert E. Bushnell.

Sidney O. Johnson, Jr., Associate Solicitor, of Arlington, Virginia, argued for the Director of the U.S. Patent and Trademark Office. With him on the brief were John M. Whealan, Solicitor, and Raymond T. Chen, Associate Solicitor. Of counsel were Maximilian R. Peterson and Mark Nagumo, Associate Solicitors.

Appealed from: Patent & Trademark Office
Board of Patent Appeals and Interferences

United States Court of Appeals for the Federal Circuit

00-1158
(Serial No. 07/631,240)

IN RE SANG-SU LEE

DECIDED: January 18, 2002

Before NEWMAN, CLEVENGER, and DYK, Circuit Judges.

NEWMAN, Circuit Judge.

Sang-Su Lee appeals the decision of the Board of Patent Appeals and Interferences of the United States Patent and Trademark Office, rejecting all of the claims of Lee's patent application Serial No. 07/631,210 entitled "Self-Diagnosis and Sequential-Display Method of Every Function."[1] We vacate the Board's decision for failure to meet the adjudicative standards for review under the Administrative Procedure Act, and remand for further proceedings.

The Prosecution Record

Mr. Lee's patent application is directed to a method of automatically displaying the functions of a video display device and demonstrating how to select and adjust the functions in order to facilitate response by the user. The display and demonstration are achieved using

computer-managed electronics, including pulse-width modulation and auto-fine-tuning pulses, in accordance with procedures described in the specification. Claim 10 is representative:

> 10. A method for automatically displaying functions of a video display device, comprising:
>
> determining if a demonstration mode is selected;
>
> if said demonstration mode is selected, automatically entering a picture adjustment mode having a picture menu screen displaying a list of a plurality of picture functions; and
>
> automatically demonstrating selection and adjustment of individual ones of said plurality of picture functions.

The examiner rejected the claims on the ground of obviousness, citing the combination of two references: United States Patent No. 4,626,892 to Nortrup, and the Thunderchopper Helicopter Operations Handbook for a video game. The Nortrup reference describes a television set having a menu display by which the user can adjust various picture and audio functions; however, the Nortrup display does not include a demonstration of how to adjust the functions. The Thunderchopper Handbook describes the Thunderchopper game's video display as having a "demonstration mode" showing how to play the game; however, the Thunderchopper Handbook makes no mention of the adjustment of picture or audio functions. The examiner held that it would have been obvious to a person of ordinary skill to combine the teachings of these references to produce the Lee system.

Lee appealed to the Board, arguing that the Thunderchopper Handbook simply explained how to play the Thunderchopper game, and that the prior art provided no teaching or motivation or suggestion to combine this reference with Nortrup, or that such combination would produce the Lee invention. The Board held that it was not necessary to present a source of a teaching, suggestion, or motivation to combine these references or their teachings. The Board stated:

> The conclusion of obviousness may be made from common knowledge and common sense of a person of ordinary skill in the art without any specific hint or suggestion in a particular reference.

Board op. at 7. The Board did not explain the "common knowledge and common sense" on which it relied for its conclusion that "the combined teachings of Nortrup and Thunderchopper

would have suggested the claimed invention to those of ordinary skill in the art."

Lee filed a request for reconsideration, to which the Board responded after five years. The Board reaffirmed its decision, stating that the Thunderchopper Handbook was "analogous art" because it was "from the same field of endeavor" as the Lee invention, and that the field of video games was "reasonably pertinent" to the problem of adjusting display functions because the Thunderchopper Handbook showed video demonstrations of the "features" of the game. On the matter of motivation to combine the Nortrup and Thunderchopper references, the Board stated that "we maintain the position that we stated in our prior decision" and that the Examiner's Answer provided "a well reasoned discussion of why there is sufficient motivation to combine the references." The Board did not state the examiner's reasoning, and review of the Examiner's Answer reveals that the examiner merely stated that both the Nortrup function menu and the Thunderchopper demonstration mode are program features and that the Thunderchopper mode "is user-friendly" and it functions as a tutorial, and that it would have been obvious to combine them.

Lee had pressed the examiner during prosecution for some teaching, suggestion, or motivation in the prior art to select and combine the references that were relied on to show obviousness. The Examiner's Answer before the Board, plus a Supplemental Answer, stated that the combination of Thunderchopper with Nortrup "would have been obvious to one of ordinary skill in the art since the demonstration mode is just a programmable feature which can be used in many different device[s] for providing automatic introduction by adding the proper programming software," and that "another motivation would be that the automatic demonstration mode is user friendly and it functions as a tutorial." The Board adopted the examiner's answer, stating "the examiner has provided a well reasoned discussion of these references and how the combination of these references meets the claim limitations." However, perhaps recognizing that the examiner had provided insufficient justification to support combining the Nortrup and Thunderchopper references, the Board held, as stated supra, that a "specific hint or suggestion" of motivation to combine was not required.

This appeal followed.

Judicial Review

Tribunals of the PTO are governed by the Administrative Procedure Act, and their rulings receive the same judicial deference as do tribunals of other administrative agencies. Dickinson v. Zurko, 527 U.S. 150, 50 USPQ2d 1930 (1999). Thus on appeal we review a PTO Board's findings and conclusions in accordance with the following criteria:

5 U.S.C. §706(2) The reviewing court shall--

> (2) hold unlawful and set aside agency actions, findings, and conclusions found to be--
>
> (A) arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law;
>
> ****
>
> (E) unsupported by substantial evidence in a case subject to sections 556 and 557 of this title or otherwise reviewed on the record of an agency hearing provided by statute;

For judicial review to be meaningfully achieved within these strictures, the agency tribunal must present a full and reasoned explanation of its decision. The agency tribunal must set forth its findings and the grounds thereof, as supported by the agency record, and explain its application of the law to the found facts. The Court has often explained:

> The Administrative Procedure Act, which governs the proceedings of administrative agencies and related judicial review, establishes a scheme of "reasoned decisionmaking." Not only must an agency's decreed result be within the scope of its lawful authority, but the process by which it reaches that result must be logical and rational.

Allentown Mack Sales and Service, Inc. v. National Labor Relations Bd., 522 U.S. 359, 374 (1998) (citation omitted). This standard requires that the agency not only have reached a sound decision, but have articulated the reasons for that decision. The reviewing court is thus enabled to perform meaningful review within the strictures of the APA, for the court will have a basis on which to determine "whether the decision was based on the relevant factors and whether there has been a clear error of judgment." Citizens to Preserve Overton Park v. Volpe, 401 U.S. 402, 416 (1971). Judicial review of a Board decision denying an application for patent is thus founded on the obligation of the agency to make the necessary findings and

to provide an administrative record showing the evidence on which the findings are based, accompanied by the agency's reasoning in reaching its conclusions. See In re Zurko, 258 F.3d 1379, 1386, 59 USPQ2d 1693, 1697 (Fed. Cir. 2001) (review is on the administrative record); In re Gartside, 203 F.3d 1305, 1314, 53 USPQ2d 1769, 1774 (Fed. Cir. 2000) (Board decision "must be justified within the four corners of the record").

As applied to the determination of patentability vel non when the issue is obviousness, "it is fundamental that rejections under 35 U.S.C. §103 must be based on evidence comprehended by the language of that section." In re Grasselli, 713 F.2d 731, 739, 218 USPQ 769, 775 (Fed. Cir. 1983). The essential factual evidence on the issue of obviousness is set forth in Graham v. John Deere Co., 383 U.S. 1, 17-18, 148 USPQ 459, 467 (1966) and extensive ensuing precedent. The patent examination process centers on prior art and the analysis thereof. When patentability turns on the question of obviousness, the search for and analysis of the prior art includes evidence relevant to the finding of whether there is a teaching, motivation, or suggestion to select and combine the references relied on as evidence of obviousness. See, e.g., McGinley v. Franklin Sports, Inc., 262 F.3d 1339, 1351-52, 60 USPQ2d 1001, 1008 (Fed. Cir. 2001) ("the central question is whether there is reason to combine [the] references," a question of fact drawing on the Graham factors).

"The factual inquiry whether to combine references must be thorough and searching." Id. It must be based on objective evidence of record. This precedent has been reinforced in myriad decisions, and cannot be dispensed with. See, e.g., Brown & Williamson Tobacco Corp. v. Philip Morris Inc., 229 F.3d 1120, 1124-25, 56 USPQ2d 1456, 1459 (Fed. Cir. 2000) ("a showing of a suggestion, teaching, or motivation to combine the prior art references is an 'essential component of an obviousness holding'") (quoting C.R. Bard, Inc., v. M3 Systems, Inc., 157 F.3d 1340, 1352, 48 USPQ2d 1225, 1232 (Fed. Cir. 1998)); In re Dembiczak, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999) ("Our case law makes clear that the best defense against the subtle but powerful attraction of a hindsight-based obviousness analysis is rigorous application of the requirement for a showing of the teaching or motivation to combine prior art references."); In re Dance, 160 F.3d 1339, 1343, 48 USPQ2d 1635, 1637

(Fed. Cir. 1998) (there must be some motivation, suggestion, or teaching of the desirability of making the specific combination that was made by the applicant); In re Fine, 837 F.2d 1071, 1075, 5 USPQ2d 1596, 1600 (Fed. Cir. 1988) ("'teachings of references can be combined only if there is some suggestion or incentive to do so.'") (emphasis in original) (quoting ACS Hosp. Sys., Inc. v. Montefiore Hosp., 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984)).

The need for specificity pervades this authority. See, e.g., In re Kotzab, 217 F.3d 1365, 1371, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000) ("particular findings must be made as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed"); In re Rouffet, 149 F.3d 1350, 1359, 47 USPQ2d 1453, 1459 (Fed. Cir. 1998) ("even when the level of skill in the art is high, the Board must identify specifically the principle, known to one of ordinary skill, that suggests the claimed combination. In other words, the Board must explain the reasons one of ordinary skill in the art would have been motivated to select the references and to combine them to render the claimed invention obvious."); In re Fritch, 972 F.2d 1260, 1265, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992) (the examiner can satisfy the burden of showing obviousness of the combination "only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references").

With respect to Lee's application, neither the examiner nor the Board adequately supported the selection and combination of the Nortrup and Thunderchopper references to render obvious that which Lee described. The examiner's conclusory statements that "the demonstration mode is just a programmable feature which can be used in many different device[s] for providing automatic introduction by adding the proper programming software" and that "another motivation would be that the automatic demonstration mode is user friendly and it functions as a tutorial" do not adequately address the issue of motivation to combine. This factual question of motivation is material to patentability, and could not be resolved on subjective belief and unknown authority. It is improper, in determining whether a person of

ordinary skill would have been led to this combination of references, simply to "[use] that which the inventor taught against its teacher." W.L. Gore v. Garlock, Inc., 721 F.2d 1540, 1553, 220 USPQ 303, 312-13 (Fed. Cir. 1983). Thus the Board must not only assure that the requisite findings are made, based on evidence of record, but must also explain the reasoning by which the findings are deemed to support the agency's conclusion.

Deferential judicial review under the Administrative Procedure Act does not relieve the agency of its obligation to develop an evidentiary basis for its findings. To the contrary, the Administrative Procedure Act reinforces this obligation. See, e.g., Motor Vehicle Manufacturers Ass'n v. State Farm Mutual Automobile Ins. Co., 463 U.S. 29, 43 (1983) ("the agency must examine the relevant data and articulate a satisfactory explanation for its action including a 'rational connection between the facts found and the choice made.'") (quoting Burlington Truck Lines v. United States, 371 U.S. 156, 168 (1962)); Securities & Exchange Comm'n v. Chenery Corp., 318 U.S. 80, 94 (1943) ("The orderly function of the process of review requires that the grounds upon which the administrative agency acted are clearly disclosed and adequately sustained.").

In its decision on Lee's patent application, the Board rejected the need for "any specific hint or suggestion in a particular reference" to support the combination of the Nortrup and Thunderchopper references. Omission of a relevant factor required by precedent is both legal error and arbitrary agency action. See Motor Vehicle Manufacturers, 463 U.S. at 43 ("an agency rule would be arbitrary and capricious if the agency . . . entirely failed to consider an important aspect of the problem"); Mullins v. Department of Energy, 50 F.3d 990, 992 (Fed. Cir. 1995) ("It is well established that agencies have a duty to provide reviewing courts with a sufficient explanation for their decisions so that those decisions may be judged against the relevant statutory standards, and that failure to provide such an explanation is grounds for striking down the action."). As discussed in National Labor Relations Bd. v. Ashkenazy Property Mgt. Corp., 817 F.2d 74, 75 (9th Cir. 1987), an agency is "not free to refuse to follow circuit precedent."

The foundation of the principle of judicial deference to the rulings of agency tribunals is

that the tribunal has specialized knowledge and expertise, such that when reasoned findings are made, a reviewing court may confidently defer to the agency's application of its knowledge in its area of expertise. Reasoned findings are critical to the performance of agency functions and judicial reliance on agency competence. See Baltimore and Ohio R. R. Co. v. Aberdeen & Rockfish R. R. Co., 393 U.S. 87, 91-92 (1968) (absent reasoned findings based on substantial evidence effective review would become lost "in the haze of so-called expertise"). The "common knowledge and common sense" on which the Board relied in rejecting Lee's application are not the specialized knowledge and expertise contemplated by the Administrative Procedure Act. Conclusory statements such as those here provided do not fulfill the agency's obligation. This court explained in Zurko, 258 F.3d at 1385, 59 USPQ2d at 1697, that "deficiencies of the cited references cannot be remedied by the Board's general conclusions about what is 'basic knowledge' or 'common sense.'" The Board's findings must extend to all material facts and must be documented on the record, lest the "haze of so-called expertise" acquire insulation from accountability. "Common knowledge and common sense," even if assumed to derive from the agency's expertise, do not substitute for authority when the law requires authority. See Allentown Mack, 522 U.S. at 376 ("Because reasoned decisionmaking demands it, and because the systemic consequences of any other approach are unacceptable, the Board must be required to apply in fact the clearly understood legal standards that it enunciates in principle . . . .")

The case on which the Board relies for its departure from precedent, In re Bozek, 416 F.2d 1385, 163 USPQ 545 (CCPA 1969), indeed mentions "common knowledge and common sense," the CCPA stating that the phrase was used by the Solicitor to support the Board's conclusion of obviousness based on evidence in the prior art. Bozek did not hold that common knowledge and common sense are a substitute for evidence, but only that they may be applied to analysis of the evidence. Bozek did not hold that objective analysis, proper authority, and reasoned findings can be omitted from Board decisions. Nor does Bozek, after thirty-two years of isolation, outweigh the dozens of rulings of the Federal Circuit and the Court of Customs and Patent Appeals that determination of patentability must be based on evidence. This court

has remarked, in Smiths Industries Medical Systems, Inc. v. Vital Signs, Inc., 183 F.3d 1347, 1356, 51 USPQ2d 1415, 1421 (Fed. Cir. 1999), that Bozek's reference to common knowledge "does not in and of itself make it so" absent evidence of such knowledge.

The determination of patentability on the ground of unobviousness is ultimately one of judgment. In furtherance of the judgmental process, the patent examination procedure serves both to find, and to place on the official record, that which has been considered with respect to patentability. The patent examiner and the Board are deemed to have experience in the field of the invention; however, this experience, insofar as applied to the determination of patentability, must be applied from the viewpoint of "the person having ordinary skill in the art to which said subject matter pertains," the words of section 103. In finding the relevant facts, in assessing the significance of the prior art, and in making the ultimate determination of the issue of obviousness, the examiner and the Board are presumed to act from this viewpoint. Thus when they rely on what they assert to be general knowledge to negate patentability, that knowledge must be articulated and placed on the record. The failure to do so is not consistent with either effective administrative procedure or effective judicial review. The board cannot rely on conclusory statements when dealing with particular combinations of prior art and specific claims, but must set forth the rationale on which it relies.

Alternative Grounds

At oral argument the PTO Solicitor proposed alternative grounds on which this court might affirm the Board's decision. However, as stated in Burlington Truck Lines, Inc. v. United States, 371 U.S. 156, 168 (1962), "courts may not accept appellate counsel's post hoc rationalization for agency action." Consideration by the appellate tribunal of new agency justifications deprives the aggrieved party of a fair opportunity to support its position; thus review of an administrative decision must be made on the grounds relied on by the agency. "If those grounds are inadequate or improper, the court is powerless to affirm the administrative action by substituting what it considers to be a more adequate or proper basis." Securities & Exchange Comm'n v. Chenery Corp., 332 U.S. 194, 196 (1947). As reiterated in Federal

Election Comm'n v. Akins, 524 U.S. 11, 25 (1998), "If a reviewing court agrees that the agency misinterpreted the law, it will set aside the agency's action and remand the case -- even though the agency (like a new jury after a mistrial) might later, in the exercise of its lawful discretion, reach the same result for a different reason." Thus we decline to consider alternative grounds that might support the Board's decision.

Further Proceedings

Sound administrative procedure requires that the agency apply the law in accordance with statute and precedent. The agency tribunal must make findings of relevant facts, and present its reasoning in sufficient detail that the court may conduct meaningful review of the agency action. In Radio-Television News Directors Ass'n v. FCC, 184 F.3d 872 (D.C. Cir. 1999) the court discussed the "fine line between agency reasoning that is 'so crippled as to be unlawful' and action that is potentially lawful but insufficiently or inappropriately explained," quoting from Checkosky v. Securities & Exch. Comm'n, 23 F.3d 452, 464 (D.C. Cir. 1994); the court explained that "[i]n the former circumstance, the court's practice is to vacate the agency's order, while in the latter the court frequently remands for further explanation (including discussion of the relevant factors and precedents) while withholding judgment on the lawfulness of the agency's proposed action." Id. at 888. In this case the Board's analysis of the Lee invention does not comport with either the legal requirements for determination of obviousness or with the requirements of the Administrative Procedure Act that the agency tribunal set forth the findings and explanations needed for "reasoned decisionmaking." Remand for these purposes is required. See Overton Park, 401 U.S. at 420-221 (remanding for further proceedings appropriate to the administrative process).

VACATED AND REMANDED

[1] Ex parte Lee, No. 1994-1989 (Bd. Pat. App. & Int. Aug. 30, 1994; on reconsid'n Sept. 29, 1999).